

OFFICE OF INFORMATION SECURITY

Authorization Requirements

Standard Operating Procedures
Version 3.18

MAY 2, 2018



Office of Information Security

Table of Contents

1. Purpose	1
2. Scope.....	1
3. <i>Authorization Prerequisites</i>	1
4. <i>Assessment & Authorization (A&A) Requirements</i>	2
4.1 Registration Requirements.....	3
4.1.1 <i>Application Registration</i>	3
4.2 Security Documentation Requirements.....	3
4.2.1 <i>System Security Plan (SSP)</i>	4
4.2.2 <i>Minor Application Self-Assessment</i>	4
4.2.3 <i>Signatory Authority</i>	4
4.2.4 <i>Risk Assessment (RA)</i>	5
4.2.5 <i>Configuration Management Plan (CMP)</i>	5
4.2.6 <i>Incident Response Plan (IRP)</i>	6
4.2.7 <i>Information Security Contingency Plan (ISCP)</i>	7
4.2.8 <i>Disaster Recovery Plan (DRP)</i>	8
4.2.9 <i>Privacy Impact Assessment (PIA)</i>	8
4.2.10 <i>Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU)</i>	9
4.2.11 <i>Secure Design Review</i>	10
4.3 Technical/Testing Requirements.....	11
4.3.1 <i>Nessus Scan / [Discovery Scan (part of Nessus scan)]</i>	11
4.3.1.1 Database Scan	13
4.3.2 Quality Code Review	13
4.3.3 <i>Secure Code Review</i>	15
4.3.4 <i>Penetration Test / Application Assessment</i>	16
4.3.5 <i>Security Configuration Compliance Data</i>	17
4.3.6 <i>Security Control Assessment (SCA)</i>	19
4.3.7 <i>Control Implementation Evidence</i>	19
4.4 Closing	20
Appendix A – FedRAMP/Cloud – VA Requirements	1
Appendix B – Authorization Requirements Quick Reference Guide	1
Appendix C – Job Aid: Security Information	1



Appendix D – Minor Applications Self-Assessment SOP.....	1
Appendix E – A&A System/Facility DRP and ISCP Requirements.....	1
Appendix F – Links/URLs/E-Mail Addresses.....	1

Document Revision History

Revision Date	Summary of Changes	Version	Author
January 2014	Initial version of SOP	1.0	OCS
April 2014	Updates made to Nessus Scan, Secure Code Review, and Security Configuration Compliance Data Requirements	1.1	OCS
June 2014	Added Security Information Job Aid to Appendix C of SOP	1.2	OCS
October 2014	Implemented reference, methodology and terminology changes; and removed the IV&V Secure Code review requirement	1.3	OCS
March 2015	Added section 3.1.6 Control Implementation Evidence	1.4	OCS
April 2015	Updated section 3.1.3 Continuous Monitoring Requirement	1.5	OCS
July 2015	Updated section 3.2.10 to include references to guidance materials on the RBD process	1.6	OCS
August 2015	Added Appendix A: Cloud/FedRAMP Reciprocity ATO Process	1.7	OCS
August 2015	Updated new compliance scan 'Report' request process location	1.8	OCS
September 2015	Updated the IRP, ISCP, and DRP sections by removing ISCPA tool references.	1.9	OCS
October 2015	Updated the IRP, ISCP, and DRP sections with minor changes.	2.0	OCS
October 2015	Updated SOP to add in Section 3.1, Registration Requirements	2.0	OCS
November 2015	Added Appendix D – A&A System/Facility DRP and ISCP Requirements. Updated the ISCP and DRP sections based on new OBC guidelines.	2.0	OCS
December 2015	Updated SCA section and added location for ISA/MOU latest templates	2.1	OCS
December 2015	Re-Added Section 3.1, Registration Requirements which was removed accidentally	2.2	OCS
January 2016	Updated section 3.3.5 (IRP). OBC is not responsible for IRPs. Removed OBC references from IRP section.	2.3	OCS
May 2016	Added VASI reference to Section 3.1.1 Application Registration	2.4	OCS
June 2016	Replaced http://go.va.gov/xxx links with functional links	2.5	OCS
June 2016	Edits throughout the document and integrated cloud-based VA applications and cloud-based third-party systems requirements	2.6	OIS
July 2016	Added Appendix E, NSOC Scanning Questionnaire information, and POA&M Management Guide reference; removed broken link from SCCD section	2.7	OCS
September 2016	Updated Code Review Continuous Monitoring requirements	2.8	OCS
October 2016	Added Minor Application Self-Assessment SOP	2.9	OCS

December 2016	Added DB scan requirement for HQ systems	3.0	OCS
January 2017	Added section 3.2.11: Secure Design Review; removed RBD section	3.1	OCS
January 2017	Updated CMP and IRP sections; also updated the POA&M Management Guide link.	3.2	OCS
February 2017	Updated the DB scan requirement and Security Configuration Compliance Data requirement sections	3.3	OCS
February 2017	Removed R6 VAKN/CDN Assessing reference from Appendix E	3.3	OCS
March 2017	Updated Section 3: Security Packages submission 45 days prior to ATO expiration date Updated Appendix A: Added new section - Other Federal Agency (Non-FedRAMP) ATO Acceptance	3.4	OCS
March 2017	Added note to Appendix A and added ISO and SO assignment requirement	3.5	OCS
March 2017	Added NEWT/REEF Reporting to section 3.3.1	3.6	OCS
April 2017	Updated section 4.2.10 (ISA/MOU)	3.7	OCS
April 2017	Updated section 4.3.6 (SCA)	3.8	OCS
April 2017	Added Scope statement	3.9	OCS
May 2017	Updated section 4.2.11 Secure Design Review; Updated the TOC to show the DB scan section 4.3.1.1	3.10	OCS
June 2017	Updated section 4.1.1; included COTS products registration requirement. Added a new section 4.3.2: Quality Code Review	3.11	OCS
July 2017	Updated links to request technical scans under section 4.3	3.12	OCS
October 2017	Added a note to Section 4; Added more details on findings remediation timeline.	3.13	OCS
December 2017	Changed title to Authorization Requirements SOP Guide. Replaced “Accreditation” with “Authorization” throughout the document. Added link for Nessus scan requests in section 4.3.1 Step 2.	3.14	OCS
January 2018	Updated Security Configuration Compliance Data (SCCD) guidance in section 4.3.5, Appendix B, and Appendix F Updated verbiage in Section 4.3 requiring SOs/Delegates to upload an explanation for any technical requirement that’s considered not applicable	3.15	OCS
March 2018	Updated verbiage in section 3.3 indicating SO or delegate should work with ISO to review authorization requirements Added link for new Major Change Notification Form requirement under section 4	3.16	OCS
April 2018	Removed links in Appendix F that are no longer active	3.17	OCS
May 2018	Updated inactive links	3.18	OCS

1. Purpose

To obtain and maintain a VA Authority-to-Operate (ATO), the authorization requirements included within the contents of this document must be completed. RiskVision, VA's Governance, Risk and Compliance (GRC) tool is the authoritative management tool for the VA Assessment and Authorization (A&A) process and Risk Management Framework. All systems will be assessed in RiskVision by an OCS representative [Certification Agent (CA)] for an authorization recommendation to be submitted to the OIS Chief Information Security Officer (CISO) and VA Chief Information Officer (CIO) [Authorizing Official] for final ATO consideration.

RiskVision guidance documentation can be found on the [Office of Information Security \(OIS\) Portal](#). The [Assessment & Authorization Requirements](#) section of this document outlines the technical/testing and security documentation requirements necessary to support an authorization decision. In addition to the descriptions and procedures in this document, the authorization requirements are listed in the [Authorization Requirements Quick Link Reference Guide](#) located on the OIS Portal and in [Appendix A](#) of this document.

This is a living document based on current federal and VA security policies, standards and guidance, and is subject to change.

2. Scope

These procedures apply to systems that are required to obtain an Authority to Operate (ATO). It does not apply to sandbox environments, non-VA networks, or development networks not otherwise connected to the VA network. Those environments will be excluded from the procedures identified in this SOP. They will not be entered into GRC and thus any documentation to include POAMs would not be loaded into GRC and GRC would not be the appropriate tracking mechanisms for deficiencies.

3. Authorization Prerequisites

The following steps need to be followed once a system is identified as needing a VA authorization decision:

1. Designate an ISO to the project. If an ISO is not yet assigned, complete the following steps:
 - a) System Owner or delegate completes the [Request For Information Security Officer Support Form](#) and e-mail to VAFSSISORRequests@va.gov.
 - b) The FSS ISO work group will coordinate an ISO assignment to help the project team assist with authorization requirements and participate with information security requirements throughout the System Development Life Cycle (SDLC).
2. Create a RiskVision entry of the Application or System by completing the following steps:

- a) System Owner or delegate completes the RV System Inventory Checklist vX.X (available upon request) provided by the ISO or from the RiskVision Working Group (RVWG) VARiskVisionWG@va.gov.
 - b) The RVWG will include the Application/System for discussion on the weekly meeting agenda, scheduled Thursdays at 12:00pm EST. During the meeting, RVWG can approve or deny the Application/System or request additional information before a decision.
 - c) Once RVWG approves the Application/System for a RiskVision entry, the System Owner or delegate will be notified by OCS via e-mail from the GRC Service Desk (vaGRCservicedesk@va.gov) stating access to the applicable instance of RiskVision:
 - National Release GRC Instance: <https://vawww.grc.va.gov/spc/index.jsp>
 - Enterprise Operations GRC Instance: <https://vawww.eogrc.va.gov/spc/index.jsp>
3. Once the applicable parties have access to RiskVision and the system resides in the tool, the System Owner or delegate shall contact their ISO to review the authorization requirements and determine if certain requirements are not applicable based on the type of system in question.

The applicable system POCs must have their authorization package completed and uploaded to RiskVision no less than 45 calendar days prior to the date they want their authorization decision to be made.

4. Assessment & Authorization (A&A) Requirements

The VA A&A requirements include technical/testing, security documentation, and security control compliance requirements. Details about the various requirements are in the following sections.

Authorization packages must be completed and uploaded to RiskVision no less than forty-five (45) calendar days prior to ATO decision consideration deadline. If a required security control is not implemented, the project team must create a POA&M/Finding in RiskVision to keep track of the remediation effort.

Note: *Only completed, required A&A security artifacts including the technical scan results and remediation strategies should be uploaded to Documents tab within RiskVision. Documents tab is not the place to upload evidence.*

If a system undergoes a significant (major) change (as defined below) after an ATO determination is made, it is required to re-complete the A&A requirements, including updating all security documentation to reflect the change. Additionally, the Major Change Notification Form, which can be found [here](#), must be completed and uploaded to RiskVision 45 days prior to the implementation of the major change.

Significant Change Definition: *Per the current 'draft' VA Handbook 6500.3, Assessment, Authorization, And Continuous Monitoring of VA Information Systems, the definition of 'significant change' is as follows: A significant (major) change to an information system or environment of operation is a change that is likely to affect the security state of the information system. Significant changes to an information system may include, but are not limited to, for example: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports,*

protocols, or services; (iii) installation of a new or upgraded hardware platform; (iv) modifications to cryptographic modules or services; or (v) modifications to security controls. Examples of significant changes to the environment of operation may include, but are not limited to, for example: (i) moving to a new facility; (ii) adding new core missions or business functions; (iii) acquiring specific and credible threat information that the organization is being targeted by a threat source; or (iv) establishing new/modified laws, policies, or regulations. Source: SP 800-37 Rev 1 [VA Adopted].

4.1 Registration Requirements

The following section provides details on each of the registration requirements including a description of the requirements and the parties/OIS organization(s) that will assist in the completion of the requirements.

4.1.1 Application Registration

Custom developed and COTS VA applications are required to be registered with the VA Software Assurance Program Office. Registration is necessary to maintain an inventory of the total population of VA custom and COTS applications, by type and business line according to the VA Common Application Enumeration (CAE) at [Common Application Enumeration](#) to ensure application-level security considerations are taken into account when determining readiness and performance.

For detailed instructions on the registration process, reference the VA Software Assurance Program Office procedures that can be found on the [VA Software Assurance Developer Support Site](#). More information regarding system registration in VA Systems Inventory (VASI) can be found in [VA Directive 6404](#)

Note: Application registration is required before either a Secure Code Review Validation or a Penetration Test / Application Assessment can be scheduled for all applications subject to secure code review authorization requirements. Also note that Software as a Service (SaaS) should follow COTS registration procedures.

Continuous Monitoring Requirement – Application registration is required when requested by OCS and/or NSOC.

4.2 Security Documentation Requirements

The following section provides details on each of the required security artifacts including the document requirements, references, and the parties/OIS organization(s) that can provide additional guidance for each artifact.

Templates for the applicable security artifacts/documents mentioned below are available on the OIS Portal at [A&A Home Documents](#). Contact your ISO for questions on how to complete the documentation.

Note: (Applicable to EO systems only) Artifact that is generated through RiskVision and is part of the Authorization package, and gets reviewed / approved by the ISO/SO in RiskVision workflow as part of the Authorization Package may not require signature(s) or is valid without signature(s).

4.2.1 System Security Plan (SSP)

SSP guidance is provided below:

- SSP guidance is found in NIST SP 800-18 and VA Handbook 6500.3.
- Additional guidance for completion of the SSP can be provided by OCS.
- The SSP is developed within RiskVision and a word document/template is no longer necessary.
- All required diagrams and confirmation of the security authorization boundary to include all devices and supporting software architecture should be included.
- All controls must be addressed. A finding will need to be created in RiskVision for every control that is not in place.

SSP completion steps:

1. The System Steward completes the assessments in RiskVision and develops findings and responses in the **Findings** tab for controls not in place.
2. The ISO validates information added by the System Steward in RiskVision.
3. The ISO, System Owner or delegate/System Steward exports the SSP from RiskVision and uploads the document to the **Documents** tab in RiskVision.

Continuous Monitoring Requirement – The SSP must be completed on an **annual basis** or when a significant change in the system or a major change in the data occurs.

4.2.2 Minor Application Self-Assessment

All minor applications are required to complete the Minor Application Self-Assessment and upload it to Documents repository within RiskVision as an Appendix to GSS/MA SSP. Complete instructions on completing the Minor Application Self-Assessment can be found in Minor Application Self-Assessment SOP attached as [Appendix D](#). The Minor Application Self-Assessment Workbook can be found at [A&A Home Documents](#).

4.2.3 Signatory Authority

Signatory Authority guidance is provided below:

- The Signatory Authority must be signed and dated by the appropriate parties.
- Additional guidance for completion of the Signatory Authority can be provided by OCS.

Signatory Authority completion steps:

1. System Owner or delegate completes the Signatory Authority using the template provided at [A&A Home Documents](#).
2. System Owner, ISO or delegate/System Steward uploads the Signatory Authority to the **Documents** tab in RiskVision.

Continuous Monitoring Requirement – The Signatory Authority must be completed on an **annual** basis or when a significant change in the system or a major change in the data occurs.

4.2.4 Risk Assessment (RA)

RA guidance is provided below:

- System and facilities are responsible for conducting the RA.
- RA guidance is found in NIST SP 800-30.
- Additional guidance for completion of the RA can be provided by the Office of Risk Management and Incident Reporting (RMIR)/OCS.
- The RA is developed within RiskVision and a word document/template is no longer necessary.

RA completion steps:

1. The System Steward completes the assessment in RiskVision.
2. The ISO validates information added by the System Steward in RiskVision.
3. The ISO, System Owner or delegate/System Steward exports the RA from RiskVision and uploads the document to the **Documents** tab in RiskVision.

Continuous Monitoring Requirement – The RA must be updated on an **annual** basis or when a significant change in the system or a major change in the data occurs.

4.2.5 Configuration Management Plan (CMP)

CMP guidance is provided below:

- Facilities are responsible for completing the CMP (pending clarification on requirement for systems)
- CMP guidance can be found in NIST SP 800-128 and VA Handbook 6500.
- Additional guidance for completion of the CMP can be provided by OCS.
- The CMP should include processes for managing configuration and change management.
- The CMP should include infrastructure devices and baseline configurations (e.g., switches, routers, firewalls).

- The CMP should include a configuration file for each operating system(s), database(s), application(s), and network device(s) to validate compliance with baseline configuration.

CMP completion steps:

1. System Owner or delegate completes the CMP using the template provided at [A&A Home Documents](#).
2. ISO, System Owner or delegate/System Steward uploads the CMP to the **Documents** tab in RiskVision.

Continuous Monitoring Requirement – The CMP must be updated on an **annual** basis or when a significant change in the system or a major change in the data occurs.

4.2.6 Incident Response Plan (IRP)

IRP guidance is provided below:

- Facilities are responsible for completing the IRP
- An IRP is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.
- IRP guidance can be found in NIST SP 800-61.
- Tools and websites that can be useful in IRP creation:
 - [Agilience RiskVision Enterprise Operations GRC Instance](#)
 - [Agilience RiskVision National Release GRC Instance](#)
 - [Office of Cyber Security \(OCS\) Portal](#)
- The System Owner works with the assigned ISO to create the IRP.
- Once completed and tested, the System Owner or designee uploads the signed IRP into RiskVision.
- Each site is responsible for developing local level procedures incorporating VA-NSOC areas of responsibility.

IRP completion steps:

1. The following inputs must be used in IRP creation:
 - RA
 - SSP
2. Must meet the following standards in IRP creation:
 - [Information Access and Privacy Program](#)
 - [NIST Special Publication 800-61 - Computer Security Incident Handling Guide](#)
 - [VA Handbook 6500.3, Certification and Authorization of Federal Information Systems](#)

Continuous Monitoring Requirement – The IRP must be tested and updated on an **annual** basis or when a significant change in the system or a major change in the data occurs.

4.2.7 Information Security Contingency Plan (ISCP)

ISCP guidance is provided below:

- ISCP plan is expected for each “Assessing” entity as identified in GRC
- ISCP plan is also expected for all LAN entities (the term “LAN” speaks to the facility boundary) within each facility including PBX (may only apply to certain facilities with wired PBX) and/or MA (may only apply to facilities that house and manage the MA)
- In accordance with the FY16 action item, all sites are required to update their ISCPs, and plans must be tested
- Contingency planning refers to interim measures to recover information system services after a disruption
- All plans must reflect the current environment and must be completed using the approved FY16 OBC template
- The System Owner or delegate develops or revises the Information System Contingency Plan.
- The System Owner or designee uploads the Information System Contingency Plan into RiskVision.
- Additional guidance for completion of the ISCP can be provided by the OBC or by visiting [Business Continuity Portal](#).
- Tools and websites that can be useful in ISCP creation:
 - [Agilance RiskVision Enterprise Operations GRC Instance](#)
 - [Agilance RiskVision National Release GRC Instance](#)
 - [Business Continuity Portal](#)
 - [Office of Cyber Security \(OCS\) Portal](#)

ISCP completion steps:

1. The ISCP template can be found [here](#).
2. The following inputs must be used in the ISCP creation:
 - Preliminary Information System Contingency Plan
 - Primary Site System Security Plan
 - Backup Site System Security Plan
3. Must meet the following standards in ISCP creation:
 - [NIST Special Publication 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems](#)
 - [Office of Information Security, Authorization Requirements Guide Standard Operating Procedures](#)
 - [VA Handbook 6500.8, Information System Contingency Planning](#)

Continuous Monitoring Requirement – The ISCP must be tested and updated on an **annual** basis or when a significant change in the system or a major change in the data occurs.

4.2.8 Disaster Recovery Plan (DRP)

DRP guidance is provided below:

- A DRP is required for each facility hosting the system components
- For Region 1 – 6 , facility DRPs (collectively) cover the Region DRP requirement
- For Region Other, each “Assessing” entity must have a DRP
- In accordance with the FY16 action item, all sites are required to update their DRPs, and plans must be tested.
- All plans must reflect the current environment and must be completed using the approved FY16 OBC template.
- The System Owner or designee develops the DRP as the entry point for the creation of both the facility and data center plans.
- Once completed (and tested), the System Owner or designee uploads the DRP into RiskVision.
- Additional guidance for completion of the DRP can be provided by OBC or by visiting [Business Continuity Portal](#).
- Tools and websites that can be useful in DRP creation:
 - [Agilience RiskVision Enterprise Operations GRC Instance](#)
 - [Agilience RiskVision National Release GRC Instance](#)
 - [Business Continuity Portal](#)
 - [Office of Cyber Security \(OCS\) Portal](#)

DRP completion steps:

1. The DRP template can be found [here](#).
2. The following inputs must be used in DRP creation:
 - Primary Site System Security Plan
 - Backup Site System Security Plan
3. Must meet the following standard in DRP creation:
 - [Office of Information Security, Authorization Requirements Guide Standard Operating Procedures](#)

Continuous Monitoring Requirement – The DRP must be tested and updated on an **annual** basis or when a significant change in the system or a major change in the data occurs.

4.2.9 Privacy Impact Assessment (PIA)

PIA guidance is provided below:

- A complete PIA must have:
 - A previously completed Privacy Threshold Analysis (PTA).

- Been completed in the most up-to-date and Privacy Services approved template for both the PTA and PIA. The PTA and PIA template can be found at [A&A Home Documents](#).
- Been completed in coordination with the VA Privacy Services Office.
- Been signed by the System Owner, Privacy Officer, and ISO.
- Been re-submitted whenever there are significant (major) changes to the system or within 3 years.
- Authority is found in E-Government Act of 2002, OMB Circular 03-22, VA Directive 6502, VA Directive 6508, and VA Handbook 6508.1.
- Additional guidance for completion of the PIA/PTA can be provided by the Privacy Services Office. Any questions may be sent to PIASupport@va.gov.

PIA completion steps:

1. System Owner, Privacy Officer, and ISO work together to submit a PTA, which is reviewed by the Privacy Services Office.
2. After review and determination by analysts, the PTA must be signed by the System Owner, Privacy Officer, ISO, and any other relevant stakeholders and re-submitted to the Privacy Services Office via PIASupport@va.gov.
3. If a PIA is required as an outcome of the PTA analysis by the Privacy Services Office, a PIA must be completed and submitted to the Privacy Services Office and then comments by the analysts, if any, must be incorporated.
4. Once the PIA is verified as complete by Privacy Services, re-submit the PIA as a PDF file with the signatures of the System Owner, Privacy Officer, ISO, and any other relevant stakeholders to PIASupport@va.gov.
5. The PIA must then be uploaded into the GRC tool as an artifact. System Owner or delegate/System Steward uploads the PIA to the **Documents** tab in RiskVision.

Continuous Monitoring Requirement – A PTA must be submitted every year. The PIA is valid for 3 years if there are no significant changes to the system.

4.2.10 Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU)

ISA/MOU guidance is provided below:

- Before an external connection can be granted, a Memorandum of Understanding (MOU) and an Interconnection Security Agreement (ISA) are required to authorize a connection between information systems that do not share the same Authorizing Official.
- An ISA/MOU must be provided for all external interconnections.
- ISA/MOU guidance can be found in NIST SP 800-47 and VA Handbook 6500.

- Additional guidance for completion of the ISA/MOU can be found in the Field Security Service (FSS) Bulletin # 269 or by contacting the Health Information Security Division at vafsshisd@va.gov or the OIT Enterprise Risk Management (ERM) CRISP Team at Sharon.mcallister@va.gov.

ISA/MOU completion steps:

1. System Owner in coordination with the entities identified in NIST SP 800-47 will complete the ISA/MOU using the latest template provided at: [OIS Portal](#) or [A&A Home Documents](#).
2. ISO will upload all final draft MOU/ISA documents to the MOU/ISA Review Submissions SharePoint site for a review prior to requesting signatures.
3. A VA review team will assess the documents against a checklist for quality and content.
4. The reviewer and the ISO will work collaboratively to correct deficiencies found in the documentation.
5. The reviewer will notify the ISO via email informing them that the document is ready for signatures.
6. The ISO will process the document for signature.
7. Upon receipt of the completed and signed MOU/ISA document, the ISO will upload the document to the Enterprise Document SharePoint.
8. The finalized document should also be added to the existing A&A artifacts in RiskVision.

Continuous Monitoring Requirement – The ISA/MOU Review Sheet must be completed on an **annual** basis. If there is a significant change, which impacts the architecture, please contact the Health Information Security Division at vafsshisd@va.gov to determine if an update to the ISA/MOU is necessary.

4.2.11 Secure Design Review

Secure Design Review (Application Threat Modeling) guidance is provided below:

- Secure Design Review guidance is found in [VA Secure Design Review SOP](#).
- Additional guidance for performing Secure Design Review are posted on the VA Software Assurance (SwA) Program Office [Resource Site](#)
- All required diagrams and analysis of potential threats to include all applicable technologies/libraries utilized by the custom application.
- All potential threats must be analyzed. A finding will need to be created in RiskVision for every potential threat that is not analyzed.

Secure Design Review completion steps:

1. The steps to request the development of an initial threat model to analyze can be found [here](#).
2. Must meet the following standards in performing this activity:
 - [VA Secure Design Review SOP](#)

3. The ISO, System Owner or delegate/System Steward uploads the analyzed threat model to the **Documents** tab in RiskVision.

Continuous Monitoring Requirement – The Secure Design Review must be updated on an **annual basis** or when a significant change in the system or a major change in the application architecture occurs.

4.3 Technical/Testing Requirements

The following section provides details on each of the technical/testing requirements including a description of the requirements and the parties/OIS organization(s) that will assist in the completion of the requirements. If a technical/testing requirement is not applicable, then the System Owner/Delegate needs to upload a word document to the Documents tab within RiskVision explaining why the specific technical/testing requirement is not applicable.

The links to [NSOC Supplemental Scan Request \(Vulnerability and Compliance\)](#), [NSOC Database Scan Questionnaire](#), and [NSOC Penetration Test & WASA Questionnaire](#) can be found at [NSOC Scan Documents](#). Additionally, the necessary information and step-by-step instruction for developing, maintaining, reporting and monitoring weaknesses as it relates to a specific system can be found in the [POA&M Management Guide](#).

Findings identified in each technical scan should be mitigated within the remediation timeframe specified in the VA Handbook 6500, (i.e.) Critical – 30 days; High – 60 days; Moderate – 90 days; Low – determined by the System Owner; Emergent – ASAP. One finding should be created in RiskVision for each of the applicable scans to track the remediation progress. In addition, well documented remediation strategy with expected remediation date and status of each finding should also be uploaded to Documents tab within RiskVision for each of the applicable scan.

4.3.1 Nessus Scan / [Discovery Scan (part of Nessus scan)]

A credentialed vulnerability scan against all instances of the operating system and desktop configurations must be conducted to identify security flaws. When conducting the Nessus Scan, a discovery scan to identify all assets within the authorization boundary must be conducted as a part of the vulnerability scan (a discovery scan will not enumerate any vulnerabilities). All Critical and High deficiencies should be mitigated with documented mitigation evidence provided, and Moderate and Low deficiencies should be mitigated or have a documented mitigation plan. This mitigation plan should include a timetable for mitigation of Moderate and Low deficiencies.

If a system's Nessus Scan data is not currently displayed in the Threat & Vulnerability Manager (TVM) within RiskVision, refer to the TVM guidance material located on the OIS portal at [Training and Brown Bag Materials](#) site for detailed information on how to access TVM.

The following steps must be performed to meet the Nessus Scan requirement (if the Nessus Scan data is included in TVM, skip to [Step 3](#)):

1. If the system receives a monthly predictive Nessus vulnerability scan from NSOC and the IP addresses that make up the system are all Windows based then please provide the IP Ranges to the CPO at CertificationPMO@va.gov, so the applicable Nessus data can be provided in TVM within RiskVision, then proceed to Step 3.
 - a) If the system receives a monthly predictive Nessus vulnerability scan from NSOC, and the IP addresses that make up the system are not all Windows based, then proceed step 2, as all necessary Operating System information will not be captured in the predictive scans from NSOC that are filtered into TVM.
 - b) If the IP addresses that make up a system are outside of the VA network (Managed Services) and/or the system does not currently receive a monthly predictive Nessus vulnerability scan from NSOC, then proceed to Step 2.
2. System Owner or delegate can request a Nessus scan using this [link](#). Once the request is completed, CPO will work with NSOC to determine if a separate supplemental vulnerability scan shall be conducted or authentication information for the non-Windows devices be added to the existing monthly predictive scan. If a separate supplemental scan is decided on by CPO/NSOC, upload the results to the **Documents** tab within RiskVision when results are sent to you or if its decided that the authentication information can be added for the non-Windows devices to the monthly predictive scans conducted by NSOC then please provide the IP Ranges to the CertificationPMO@va.gov, so the applicable Nessus data can be provided in TVM within RiskVision.
 - a) Note: NSOC must conduct an independent Nessus Scan for all VA owned systems and Managed Services. NSOC has visibility into Enterprise Operations (EO) systems and has the ability to perform Nessus scans in coordination with system personnel if needed. External systems / Managed Services must have a recent NSOC Nessus scan conducted either via remote connection or by utilizing NSOC staff on-site to perform scans, when necessary.
3. Once the system's Nessus Scan data is accurately shown in TVM within RiskVision, System Owner or delegate follows these steps:
 - a) Browse to [Nessus Enterprise Web Tool \(NEWT\)](#) and use the Remediation Effort Entry Form (REEF) to document your manual remediation effort. For each deficiency identified from the scan, the System Owner or delegate creates a response within REEF for mitigating the deficiencies and / or provides evidence that the deficiencies have been mitigated. Also, include the scheduled completion date and status of each deficiency within REEF.
 - b) Once all manual remediation has been documented within REEF, run this report https://spsites.cdw.va.gov/sites/FODW_PVT/Progress%20Reports/Progress_ReportbyRegion_Chart.rdl within NEWT.
 - c) Export the report by going to the upper left side of the screen select the Actions Menu. Choose Export and select Excel. Save the file.
 - d) System Owner or delegate then uploads the report from step 3 above to the Documents tab within RiskVision. Mitigation information can also be provided in the Vulnerabilities tab within RiskVision.

- e) Within the uploaded mitigation strategy, each system should conduct an analysis on the results of the vulnerability scans to determine and document those findings that are false positives, not applicable to the system, or otherwise mitigated. Additionally, findings that must be remediated through or from the vendor should also be documented as part of this analysis.

Note: If Nessus Scan data is not currently provided in TVM for the system and instead raw Nessus Scan results exist from NSOC, the System Owner or delegate shall upload the actual Nessus Scan results to the Documents tab in RiskVision; along with a mitigation strategy for each finding. Also, within NEWT, if the ISO/System Owner does not have an option to pull a report for their FISMA reportable system, then contact the VA GRC Service Desk to provide the IP address range of the system authorization boundary to add it to NEWT to pull the report.

4. System Owner or delegate creates one finding and a response in the **Findings** tab within RiskVision for the Nessus scan to serve as a reminder to resolve the deficiencies.

Note: A follow-up Nessus scan may be requested by OIS to ensure deficiencies have been mitigated and new deficiencies do not exist as part of the ongoing authorization process.

Continuous Monitoring Requirement – NSOC conducts predictive Nessus vulnerability scans on a **monthly** basis. A supplemental scan is required for A&A purposes when requested by OCS, NSOC, and/or when new vulnerabilities potentially affecting the system/applications are identified and reported. To maintain the authorization decision, the system must meet this continuous monitoring requirement.

4.3.1.1 Database Scan

Both HQ and EO systems must request a database scan if the project hosts a database to store and process information. A database scan must be conducted at least on an annual basis. In order to maintain the authorization decision for the system, any findings must be remediated within the approved timelines for the severity of the findings, and a POA&M must be created in RiskVision to keep track of the remediation effort. Database scans can be requested by visiting this [link](#). The database scanning team can also be reached at VANSOCDBScans@va.gov for more information. If a database scan is not applicable, upload a word document to the Documents tab within RiskVision explaining why a database scan is not applicable.

4.3.2 Quality Code Review

Quality code reviews of custom developed VA applications using the approved VA static code analysis tool should be conducted to identify code quality issues within VA applications. Applications written in languages that are not supported, such as MUMPS, shall be targeted for manual review of testing with other applicable tools; notify the VA Software Assurance (SwA) Program Office if this is the case at: OISSwASupportGroup@va.gov. If a Quality Code Review is not applicable, upload a word document to the Documents tab within RiskVision explaining why a Quality Code Review is not applicable.

For detailed instructions on the code reviews process, reference the VA Quality Code Review SOP and guidance materials, which are posted on the [VA SwA Program Office Resource](#) Site. An overview of the quality code review instructions are provided below.

Verification & Validation (V&V) Quality Code Reviews

V&V quality code reviews are conducted during the development or maintenance of a VA application by the VA Application Development team. Close cooperation between OIS and the Office of Information Technology (OIT), including supporting contractors, is critical to achieving quality code review objectives and increasing the level of confidence that software developed for use at the VA is robust and maintainable. The goals of performing quality code reviews include making sure that unpredictable behavior due to poor code quality is minimized and that V&Vs performed by VA software developers are done correctly and consistently, according to minimum standards prescribed by the VA.

The following steps must be performed to meet the V&V quality code review requirement:

1. VA Application Developers open a NSD ticket [(855) NSD-HELP] to request VA static code analysis tools in order to perform scans according to the procedures in the VA Quality Code Review SOP and guidance materials.
2. VA Application Developers scan their own application source code.
3. VA Application Developers open a NSD ticket [(855) NSD-HELP] to request validation of a final V&V quality code review.
4. VA Application Developers deliver the scan results to the VA SwA Program Office at: OISSwASupportGroup@va.gov for review, work with the VA SwA Program Office to schedule the validation, and coordinate with them to resolve any issues identified during validation.
 - a) The scan results are reviewed to ensure that minimum VA standards have been met. The VA SwA Program Office determines whether additional analysis is needed, and works with the VA Application Developers to ensure that they understand how to meet the standards required.
5. System Owner or delegate uploads full test results to the Documents tab in RiskVision.
6. For each deficiency identified from the V&V quality code review, System Owner or delegate creates a response for mitigating the deficiencies and/or provides evidence that the deficiencies have been mitigated. Also, include the scheduled completion date and status of each deficiency. Information should be provided in Excel or Word format; refer to the OCS preferred template located on the OIS Portal at [A&A Home Documents](#). System Owner or delegate uploads the aforementioned document to the Documents tab in RiskVision.
7. System Owner or delegate creates one finding and a response in the Findings tab within RiskVision for the V&V quality code review to serve as a reminder to resolve the deficiencies.

Note: See also the SwA [Blog](#) for future related A&A requirement announcements.

Continuous Monitoring Requirement – A V&V Quality Code Review is required annually once the application is in sustainment OR upon discovery that the application has already been deployed to production and has not gone through the process, e.g. older applications in sustainment OR upon every major release OR when requested by OCS and/or NSOC.

4.3.3 Secure Code Review

Secure code reviews of custom developed VA applications using the approved VA static code analysis tool should be conducted to identify vulnerabilities, coding, and design flaws within VA applications. Applications written in languages that are not supported, such as MUMPS, shall be targeted for manual review of testing with other applicable tools; notify the VA Software Assurance (SwA) Program Office if this is the case at: OISSwASupportGroup@va.gov. If a Secure Code Review is not applicable, upload a word document to the Documents tab within RiskVision explaining why a Secure Code Review is not applicable.

For detailed instructions on the code reviews process, reference the VA Secure Code Review SOP and guidance materials, which are posted on the [VA SwA Program Office Resource](#) Site. An overview of the secure code review instructions are provided below.

Note: Successful completion of the secure code review authorization requirements is required before a Penetration Test / Application Assessment can be scheduled for Major Applications.

Verification & Validation (V&V) Secure Code Reviews

V&V secure code reviews are conducted during the development or maintenance of a VA application by the VA Application Development team. Close cooperation between OIS and the Office of Information Technology (OIT), including supporting contractors, is critical to achieving secure code review objectives and increasing the level of confidence that software developed for use at the VA is free from vulnerabilities. The goals of performing secure code reviews includes making sure that risk-based activities are performed in a secure manner and that V&Vs performed by VA software developers are done correctly and consistently, according to minimum standards prescribed by the VA.

The following steps must be performed to meet the V&V secure code review requirement:

1. VA Application Developers open a NSD ticket [(855) NSD-HELP] to request VA static code analysis tools in order to perform scans according to the procedures in the VA Secure Code Review SOP and guidance materials.
2. VA Application Developers scan their own application source code.
3. VA Application Developers open a NSD ticket [(855) NSD-HELP] to request validation of a final V&V secure code review.
4. VA Application Developers deliver the scan results to the VA SwA Program Office at: OISSwASupportGroup@va.gov for review, work with the VA SwA Program Office to schedule the validation, and coordinate with them to resolve any issues identified during validation.
 - a) The scan results are reviewed to ensure that minimum VA standards have been met. The VA SwA Program Office determines whether additional analysis is needed, and works with the VA Application Developers to ensure that they understand how to meet the standards required.
5. System Owner or delegate uploads full test results to the **Documents** tab in RiskVision.

6. For each deficiency identified from the V&V secure code review, System Owner or delegate creates a response for mitigating the deficiencies and/or provides evidence that the deficiencies have been mitigated. Also, include the scheduled completion date and status of each deficiency. Information should be provided in Excel or Word format; refer to the OCS preferred template located on the OIS Portal at [A&A Home Documents](#). System Owner or delegate uploads the aforementioned document to the **Documents** tab in RiskVision.
7. System Owner or delegate creates one finding and a response in the **Findings** tab within RiskVision for the V&V secure code review to serve as a reminder to resolve the deficiencies.

Note: See also the SwA [Blog](#) for future related A&A requirement announcements.

Continuous Monitoring Requirement – A V&V Secure Code Review is required annually once the application is in sustainment OR upon discovery that the application has already been deployed to production and has not gone through the process, e.g. older applications in sustainment OR upon every major release OR when requested by OCS and/or NSOC.

4.3.4 Penetration Test / Application Assessment

A penetration test or full application assessment must be performed that includes automated and manual assessment tools and techniques on Internet Facing and/or High Impact Systems. All Critical and High deficiencies should be mitigated with documented mitigation evidence provided, and Moderate and Low deficiencies should be mitigated or have a documented mitigation plan. If a Penetration Test / Application Assessment is not applicable, upload a word document to the Documents tab within RiskVision explaining why a Penetration Test / Application Assessment is not applicable. **The Penetration Test / Application Assessment requirement is not applicable to Vista systems.*

The following steps must be performed to meet the Penetration Test/Application Assessment requirement:

1. System Owner or delegate can request a penetration test/application assessment by completing the *NSOC Penetration Test Questionnaire / NSOC WASA Questionnaire* found at [NSOC Scan Documents](#) to request penetration test/application assessment from NSOC. Please allow 30 days for NSOC to schedule/conduct the penetration test/application assessment.
 - a) NSOC must conduct an independent penetration test/application assessment for all VA owned applications and Managed Services. NSOC must have visibility into all VA applications where an authorization decision is required. External systems must also have a recent NSOC penetration test/application assessment performed either remotely or by utilizing NSOC staff on-site to perform scans, when necessary.
2. NSOC will provide results to system POCs.
3. System Owner or delegate uploads actual results to the **Documents** tab in RiskVision.
4. For each deficiency identified from the penetration test/application assessment, the System Owner or delegate creates a response for mitigating the deficiencies and/or provides evidence that the deficiencies have been mitigated. Also include the scheduled completion date and status

of each deficiency. Information should be provided in Excel or Word format; refer to the OCS preferred template located on the OIS Portal at [A&A Home Documents](#). System Owner or delegate uploads the aforementioned document to the **Documents** tab in RiskVision.

- a) Within the uploaded mitigation strategy, each system should conduct an analysis on the results of the penetration test to determine and document those findings that are false positives, not applicable to the system, or otherwise mitigated. Additionally, findings that must be remediated through or from the vendor should also be documented as part of this analysis and should be documented in either the report of findings provided from VA-NSOC or as a separate document.
5. System Owner or delegate creates one finding and a response in the **Findings** tab within RiskVision for the Penetration Test/Application Assessment to serve as a reminder to resolve the deficiencies.

Continuous Monitoring Requirement – An NSOC penetration test/application assessment is required on an annual basis to maintain an ATO and/or when a major change to the system or upgrades to the tools used occurs. In addition, OI&T conducts penetration testing **quarterly** on **one-fourth** of the total number of VA High Systems and/or internet facing systems.

4.3.5 Security Configuration Compliance Data

Security Configuration Compliance data must be obtained for all IP addresses that make up a system and must check against VA approved hardening guidance for all Operating Systems, Databases, Networks, and Security Devices, where guidance exists. If Security Configuration Compliance data is not applicable, upload a word document to the Documents tab within RiskVision explaining why Security Configuration Compliance data is not applicable.

The following steps must be performed to meet the Security Configuration Compliance requirement:

1. The System Owner or delegate contacts CPO at CertificationPMO@va.gov to ensure the IP addresses or system names that make up their system(s) are appropriately tagged or accounted for in RiskVision. The CPO office will assist the System Owner with items ‘a’ and/or ‘b’ below depending on the system.
 - a) For systems with IP address ranges internal to the VA that have the IBM Endpoint Manager (IEM) agent installed:
 - i. System Owner/Delegate should verify their IP addresses or system names by reviewing the boundaries displayed in the Enterprise Visibility and Vulnerability Management (EVVM) Dashboard.
Regional GSS boundaries can be found at: <https://dashboard.tic.va.gov/s/290/>
Facility GSS and **System** boundaries can be found at:
<https://dashboard.tic.va.gov/s/291/>

If there are any discrepancies found please send an email to the CPO (CertificationPMO@va.gov) and CC the OIS EV Support Group (OISEVSupportGroup@va.gov).

- ii. After reviewing information system boundaries for accuracy, System Owner/Delegate should run the Security Configuration Compliance Data (SCCD) **Checklist Trending** and **Compliance Trending** reports and export them to PDF from the EVVM Dashboard (<https://dashboard.tic.va.gov> > Enterprise > All Systems > Authorization & Accreditation).

Checklist Trending reports are located at:

Regional GSS: <https://dashboard.tic.va.gov/s/28T/>

Facility GSS: <https://dashboard.tic.va.gov/s/28V/>

System: <https://dashboard.tic.va.gov/s/28X/>

Compliance Trending reports are located at:

Regional GSS: <https://dashboard.tic.va.gov/s/28U/>

Facility GSS: <https://dashboard.tic.va.gov/s/28W/>

System: <https://dashboard.tic.va.gov/s/28Y/>

When running the compliance reports please select the applicable information system (Note: Both boundary data and compliance data are updated nightly).

- iii. System Owner/Delegate then uploads the Compliance Trending and Checklist Trending reports to the Documents tab in RiskVision.
 - iv. System Owner/Delegate creates one finding and a response in the Findings tab within RiskVision for the compliance scan to serve as a reminder to resolve the deficiencies.
 - v. System Owner/Delegate continues to remediate deficiencies identified from the Compliance Trending and Checklist Trending reports.
 - vi. System Owner/Delegate uploads new Compliance Trending and Checklist Trending reports to the Documents tab within RiskVision as evidence to show the remediation progress.
- b) For systems with IP address ranges external to the VA that do not have the IBM Endpoint Manager (IEM) agent installed: System Owner or delegate must submit a 'Supplemental Scan Request' form found at the [NSOC Scan Documents](#) site. Ensure that the 'Compliance' check box is checked. The CPO will submit this form to the NSOC and an NSOC POC will contact the System Owner/Administrator to schedule the compliance scan. NSOC will submit compliance results/reports to system POCs for compliance scans that are conducted. Please work with CertificationPMO@va.gov if you are not receiving these compliance reports/results.
- i. In most cases, NSOC has visibility into external Managed Services and has the ability to perform compliance scans in coordination with system personnel. External systems must have a recent NSOC compliance scan conducted either via remote connection or by utilizing NSOC staff on-site to perform scans, when necessary. In addition to this requirement, OIS may request that NSOC conduct a follow-up

compliance scan, where necessary. NSOC has the ability to provide an assessment of compliance scan results and recommendations prior to an authorization determination.

2. System Owner or Delegate uploads the Compliance Trending and Checklist Trending reports to the Documents tab in RiskVision. The Compliance Trending and Checklist Trending reports can be found at <https://dashboard.tic.va.gov/s/28U/> and <https://dashboard.tic.va.gov/s/28T/>, respectively.
3. System Owner or Delegate creates one finding and a response in the Findings tab within RiskVision for the compliance scan to serve as a reminder to resolve the deficiencies.
4. System Owner or Delegate continues to remediate deficiencies identified from the Compliance Trending and Checklist Trending reports.
5. System Owner or Delegate uploads new Compliance Trending and Checklist Trending reports to Documents tab within RiskVision as evidence to show the remediation progress.

Continuous Monitoring Requirement – An NSOC or NSOC approved Security Configuration Compliance Scan must be performed on a **quarterly** basis on external systems, or when changes are made to the approved secure configuration/hardening guides, or compliance reports must be pulled in accordance with the guidance above on a **quarterly** basis, or when changes are made to the approved secure configuration/hardening guides, or when requested by OCS.

4.3.6 Security Control Assessment (SCA)

A SCA may be required by the OCS. If an SCA is required, all Critical and High POA&Ms should be mitigated with documented mitigation evidence provided. Moderate and Low POA&Ms should be mitigated or have a documented mitigation plan.

The following steps must be performed to meet the SCA requirement:

1. Once notified by OCS that a SCA is required, the appropriate audit team will be notified by the OCS to schedule the assessment.
2. The assigned audit team will conduct the SCA.
3. OCS will create a SCA program for the appropriate entity in GRC that was audited.
4. The audit team lead will upload the deliverables, to include the SCA report and import the POAMs, within 4 weeks of completion of the audit.
5. System Owner or delegate creates responses to the POAMs/findings within 15 days of the POAMs uploaded.

Continuous Monitoring Requirement – An SCA will be performed based on the criticality of the system and/or if circumstances arise that require an onsite SCA under the discretion of OCS.

4.3.7 Control Implementation Evidence

|||||

All control implementation statements evaluated as part of the RiskVision Assessment Workflow need to contain evidence that demonstrates the control was tested, how it was tested, and the results. The evidence will be required for all controls that are documented to be in place and the results can be documented by going to the appropriate assessment and clicking on the General tab. From the General tab, select each control in the Control Test column to document how a control was tested, the results, and any associated findings.

4.4 Closing

Once all of the above requirements are either met or deemed inappropriate by OIS, the completed package will be submitted to the Authorizing Official by OCS/CA with one of the following recommendations:

- ATO
 - ATO with Conditions: An authorization decision allowing a system to operate for an established amount of time (e.g., 30, 60, 90, 120 days) if certain terms and conditions must still be met, or
 - Full ATO: An authorization decision allowing a system to operate and fall into the Continuous Monitoring process if all applicable security requirements have been met.
- Denial of ATO (DATO)
 - An authorization decision allowing the authority to halt an existing operational or new system because unacceptable security risks exist.

Appendix A – FedRAMP/Cloud – VA Requirements

FedRAMP Authorized Cloud Service Provider (CSP) Reciprocity (Agency ATO) Process

Federal Risk and Authorization Management Program (FedRAMP) is designed to assist agencies in meeting FISMA requirements for cloud systems. CSPs must meet FedRAMP in order to do business with US government agencies as part of the “Cloud first policy”. FedRAMP is designed as a “do once, use many” framework to create efficiency in government procurement of cloud services. As part of the program, CSPs pursuing FedRAMP are required to be independently assessed by a Third Party Assessment Organization (3PAO). Per the [“Acceptance of FEDRAMP Authorization Memo”](#) issued on August 11, 2015 by the Deputy Assistant Secretary for Information Security, *“existing Federal Risk and Authorization Management Program (FedRAMP) authorizations for certified FedRAMP Cloud Service Provider cloud systems should be evaluated, and reused when possible, to reduce the overall time required to grant an authorization and begin using a cloud service.”*

The Cloud/FedRAMP Reciprocity ATO process consists of the following steps:

Note: A contract must be in place before requesting a RiskVision entry of the FedRAMP Cloud Service Provider. In the absence of a contract, RVWG will not entertain any such request.

1. Designate an ISO and System Owner to the project.
2. Coordinate with the RVWG to request a RiskVision entry of the FedRAMP Cloud Service Provider. Reference section 2 (Authorization Prerequisites) for action steps.
3. System Owner and ISO will complete the CSP system questionnaire within RiskVision to define the system acronym, security categorization, operational status, system type, cloud computing service model [Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), etc.], and cloud service type (private, public, hybrid).
4. ISO will request FedRAMP repository access for CSP authorization documentation package by completing the FedRAMP [Agency Access Request Form](#) and emailing to Certification Program Office (CPO) at CertificationPMO@va.gov.
5. ISO will map the CSP authorization documentation artifacts to the VA ATO documentation requirements in RiskVision. Then review and assess the CSP’s 3PAO FedRAMP authorized SSP using the NIST/CAG-20 scoresheet provided by OCS. All documents will be uploaded to the **Documents** tab in RiskVision.
6. CSP authorization package in RiskVision will then be advanced to OCS and Certification Authority (CA) for review. Additionally, VA determines if the CSP system appropriately addresses any and all necessary VA and Department of Homeland Security (DHS) Trusted Internet Connection (TIC) requirements (e.g., all external systems, including cloud solutions, hosted from facilities or data centers outside of the VA network and boundary must comply with DHS TIC requirements and VA’s external connection agreements) before progressing to the VA CISO and Designated Accrediting Authority (DAA) for agency ATO consideration.

Cloud-Based VA Application / Workload / Third-Party System ATO Process

The Cloud/FedRAMP cloud-based VA Application / Workload / Third-Party System ATO process consists of the following steps:

1. Coordinate with the RVWG to request a RiskVision entry of the cloud-based VA Application / Workload / Third-Party System. Reference section 2 (Authorization Prerequisites) for action steps.
2. System Owner and ISO will complete the CSP/VA Application / Workload / Third-Party System questionnaire within RiskVision to define the system acronym, security categorization, operational status, system type, etc.
3. Customer Responsibilities Security Plan provided by the CSP ISO will be completed by the System Owner. This set of security controls is documented in the FedRAMP authorized CSP Customer Responsibilities Matrix. The security plan controls have been mapped to VA 6500 requirements.
4. ISO will review the completed Customer Responsibilities Security Plan for proper implementation details and uploads to the **Documents** tab in RiskVision.


The cloud-based VA Application / Workload / Third-Party System in RiskVision will then be advanced to OCS and Certification Authority (CA) for review before progressing to the VA CISO and Designated Accrediting Authority (DAA) for agency ATO consideration.

Other Federal Agency (Non-FedRAMP) ATO Acceptance

The cybersecurity requirements for VA information systems will be managed through the Risk Management Framework (RMF) consistent with the principals established in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37. Reciprocal acceptance of other federal agency system authorizations will be implemented to the maximum extent possible. Refusals must be timely, documented, and reported to the responsible VA Authorizing Official.

VA employees and contract staff working for the VA are prohibited from sending VA data outside the VA Network without an Authority to Operate signed by the VA Authorizing Official.


1. Any project seeking to use another federal agency ATO must contact the CertificationPMO@va.gov to initiate the process.
2. A review of the other agency ATO process will be initiated to ensure it meets VA requirements for NIST 800-53 implementation; ATO package review is allowed; and POAM management and tracking is in place. In the event the other agency will not share the entire A&A package, negotiations will ensue between VA and the other agency to obtain an agreed upon subset of the required documentation.

- 
3. Once an agreement/understanding is in place to review the other agency package, an entry in RiskVision will be created using the VA 6500.3 Contractor/FedRAMP program.
 4. The other Federal Agency ATO memo, along with additional documentation, will be uploaded to the documents tab in RiskVision. Additional documentation may include a list of open POAMs, required artifacts, Interconnection Security Agreements (ISA)/Memorandum of Understanding (MOU).
 5. Questionnaires will be answered and any customer responsible controls, if necessary, will be completed and uploaded to the documents tab.
 6. The workflow will be progressed to the VA Authorizing Official for review and approval.
 - If the VA AO refuses reciprocity of the other agency ATO, a memo will be developed and sent to the VA project staff for notification.

Appendix B – Authorization Requirements Quick Reference Guide

Authorization Requirements		
Requirement	Roles / Responsibilities	References
Technical/Testing Requirements		
<div> <input type="checkbox"/> </div> <p>Nessus Scan</p> <ul style="list-style-type: none"> • A <u>credentialed</u> vulnerability scan against all instances of the operating system and desktop configurations must be conducted to identify security flaws. • Actual scan results must be provided for analysis. • All Critical and High deficiencies should be mitigated with documented mitigation evidence provided, and Moderate and Low deficiencies should be mitigated or have a documented mitigation plan. • Within the uploaded mitigation strategy, each system should conduct an analysis on the results of the vulnerability scans to determine and document those findings that are false positives, not applicable to the system, or otherwise mitigated. Additionally, findings that must be remediated through or from the vendor should also be documented as part of this analysis and should be documented. • Refer to the Threat & Vulnerability Manager (TVM) guidance material located on the OIS portal at Training and Brown Bag Materials for detailed information on how to access TVM within RiskVision. 	<p>If the system's Nessus Scan data is currently displayed in TVM within RiskVision:</p> <ul style="list-style-type: none"> • Browse to Nessus Enterprise Web Tool (NEWT) and use the Remediation Effort Entry Form (REEF) to document your manual remediation effort. For each deficiency identified from the scan, the System Owner or delegate creates a response within REEF for mitigating the deficiencies and / or provides evidence that the deficiencies have been mitigated. Also, include the scheduled completion date and status of each deficiency within REEF. • Once all manual remediation has been documented within REEF, run this report https://spsites.cdw.va.gov/sites/FODW_PVT/Progress%20Reports/Progress_ReportbyRegion_Chart.rdl within NEWT. • Export the report by going to the upper left side of the screen select the Actions Menu. Choose Export and select Excel. Save the file. • System Owner or delegate then uploads the report from step 3 above to the Documents tab within RiskVision. Mitigation information can also be provided in the Vulnerabilities tab within RiskVision. • Within the uploaded mitigation strategy, each system should conduct an analysis on the results of the vulnerability scans to determine and document those findings that are false positives, not applicable to the system, or otherwise mitigated. 	<ul style="list-style-type: none"> • Contact the Office of Cyber Security (OCS) at: CertificationPMO@va.gov with any questions. • TVM guidance material located on the OIS portal at Training and Brown Bag Materials

		<p>Additionally, findings that must be remediated through or from the vendor should also be documented as part of this analysis.</p> <p>If the system's Nessus Scan data is not currently displayed in TVM within RiskVision:</p> <ul style="list-style-type: none"> • : If Nessus Scan data is not currently provided in TVM for the system and instead raw Nessus Scan results exist from NSOC, the System Owner or delegate shall upload the actual Nessus Scan results to the Documents tab in RiskVision; along with a mitigation strategy for each finding. Also, within NEWT, if the ISO/System Owner does not have an option to pull a report for their FISMA reportable system, then contact the VA GRC Service Desk to provide the IP address range of the system authorization boundary to add it to NEWT to pull the report. • <u>System Owner or delegate</u> creates one finding and a response in the Findings tab within RiskVision for the Nessus scan to serve as a reminder to resolve the deficiencies. 	
	<p>Quality Code Review</p> <ul style="list-style-type: none"> • Quality code reviews of custom developed VA applications using the approved VA static code analysis tool should be conducted to identify code quality issues within VA applications. • Applications written in languages that are not supported, such as MUMPS, shall be targeted for manual review of testing with other applicable tools; notify the VA Software Assurance (SwA) Program Office if this is the case at: OISSwASupportGroup@va.gov. 	<p>V&V Quality Code Reviews</p> <ul style="list-style-type: none"> • <u>VA Application Developers</u> open a NSD ticket [(855) NSD-HELP] to request VA static code analysis tools in order to perform scans according to the procedures in the VA Quality Code Review SOP and guidance materials. • <u>VA Application Developers</u> scan their own application source code. • <u>VA Application Developers</u> open a NSD ticket [(855) NSD-HELP] to request validation of a final V&V quality code review. • <u>VA Application Developers</u> deliver the scan results to the VA SwA Program Office at: OISSwASupportGroup@va.gov for review, work with the VA SwA Program Office to schedule the validation, and coordinate with them to resolve any issues identified during validation. <ul style="list-style-type: none"> • The scan results are reviewed to ensure that minimum 	<ul style="list-style-type: none"> • For detailed instructions on the code reviews process, reference the VA Quality Code Review SOP and guidance materials, which are posted on the VA SwA Program Office Resource Site.

		<p>VA standards have been met. The VA SwA Program Office determines whether additional analysis is needed, and works with the VA Application Developers to ensure that they understand how to meet the standards required.</p> <ul style="list-style-type: none"> • <u>System Owner or delegate</u> uploads full test results to the Documents tab in RiskVision. • <u>System Owner or delegate</u> creates a response for mitigating the deficiencies and/or provides evidence that the deficiencies have been mitigated for each deficiency identified from the V&V quality code review. Also, include the scheduled completion date and status of each deficiency. Information should be provided in Excel or Word format; refer to the OCS preferred template located on the OIS Portal at A&A Home Documents. System Owner or delegate uploads the aforementioned document to the Documents tab in RiskVision. • <u>System Owner or delegate</u> creates one finding and a response in the Findings tab within RiskVision for the V&V quality code review to serve as a reminder to resolve the deficiencies. 	
	<p>Secure Code Review</p> <ul style="list-style-type: none"> • V&V secure code reviews of custom developed VA applications must be conducted according to the VA Secure Code Review SOP located at <p>VA SwA Program Office Resource</p> <ul style="list-style-type: none"> • V&V secure code reviews are conducted by the VA Application Developers. • Applications written in languages that are not supported, such as MUMPS, shall be targeted for manual review or testing with other applicable tools (notify OCS if this is the case at: OISSwASupportGroup@va.gov). 	<p>V&V Secure Code Reviews</p> <ul style="list-style-type: none"> • <u>VA Application Developers</u> open a NSD ticket [(855) NSD-HELP] to request VA static code analysis tools; they scan their own application source code; open a NSD ticket to request validation of a final V&V secure code review; deliver the scan results to the VA SwA Program Office at OISSwASupportGroup@va.gov for review; work with the VA SwA Program Office to schedule the validation; and coordinate with them to resolve any issues identified during validation. • <u>System Owner</u> or delegate is responsible for coordinating the mitigation of deficiencies, documenting the mitigation plans, and uploading them along with the secure code review results to RiskVision under Entity Details: Documents tab. • <u>System Owner</u> or delegate creates one finding and a response in the Findings tab within RiskVision for the 	<ul style="list-style-type: none"> • Contact the NSD Help Desk [(855) NSD-HELP] to request tools (Fortify), reviews, or technical support

		secure code review to serve as a reminder to resolve the deficiencies.	
<input type="checkbox"/>	Penetration Test/Application Assessment <ul style="list-style-type: none"> A full penetration test/application assessment must be performed that includes automated and manual assessment tools and techniques on Internet Facing and/or High Impact Systems. Actual test results must be provided for analysis. All Critical and High deficiencies should be mitigated with documented mitigation evidence provided, and Moderate and Low deficiencies should be mitigated or have a documented mitigation plan. 	<ul style="list-style-type: none"> <u>System Owner or delegate</u> contacts CPO at CertificationPMO@va.gov to request penetration test/application assessment from NSOC. <u>NSOC</u> conducts penetration test/application assessment and provides results to system POCs. Please allow 30 days for NSOC to schedule/conduct the penetration test/application assessment. <u>System Owner</u> or delegate is responsible for coordinating the mitigation of deficiencies, documenting the mitigation plans, and uploading them along with the test results to RiskVision under Entity Details: Documents tab. <u>System Owner</u> or delegate creates one finding and a response in the Findings tab within RiskVision for the penetration test/application assessment to serve as a reminder to resolve the deficiencies. 	<ul style="list-style-type: none"> Contact OCS at: CertificationPMO@va.gov with any questions
<input type="checkbox"/>	Security Control Assessment (SCA) (if applicable) <ul style="list-style-type: none"> An SCA will be required only upon request from OCS. If an SCA is required, all Critical and High POA&Ms should be mitigated with documented mitigation evidence provided, and Moderate and Low POA&Ms should be mitigated or have a documented mitigation plan. 	<ul style="list-style-type: none"> Once notified by OCS that an SCA is required, the appropriate <u>audit team</u> will be notified by OCS to schedule the assessment. The assigned <u>audit team</u> will conduct the SCA. <u>OCS</u> will create a SCA program for the appropriate entity in GRC that was audited. The <u>audit team lead</u> will upload the deliverables, to include the SCA report and import the POAMs, <u>within 4 weeks</u> of completion of the audit. <u>System Owner or delegate</u> creates responses to the POAMs/findings within <u>15 days</u> of the POAMs uploaded. 	<ul style="list-style-type: none"> Contact OCS at: CertificationPMO@va.gov
<input type="checkbox"/>	Security Configuration Compliance Data <ul style="list-style-type: none"> Compliance data must be obtained for all IP addresses that make up a system and must check against VA approved hardening guidance for all Operating Systems, Databases, Networks, and Security Devices, where guidance exists. 	For systems with IP address ranges internal to the VA that have the IBM Endpoint Manager (IEM) agent installed: <ul style="list-style-type: none"> <u>System Owner or Delegate</u> contacts CPO at CertificationPMO@va.gov to ensure the IP addresses or system names that make up their system(s) are appropriately tagged or accounted for in RiskVision. <u>System Owner or Delegate</u> should run the Security Configuration Compliance Data (SCCD) Checklist Trending 	<ul style="list-style-type: none"> Contact OCS at: CertificationPMO@va.gov and NSOC, or the Enterprise Visibility Team at: OISEVSupportGroup@va.gov with any questions Internal Compliance reports location:

		<p>and Compliance Trending reports and export them to PDF from the EVVM Dashboard.</p> <p>Checklist Trending reports are located at: Regional GSS: https://dashboard.tic.va.gov/s/28T/ Facility GSS: https://dashboard.tic.va.gov/s/28V/ System: https://dashboard.tic.va.gov/s/28X/</p> <p>Compliance Trending reports are located at: Regional GSS: https://dashboard.tic.va.gov/s/28U/ Facility GSS: https://dashboard.tic.va.gov/s/28W/ System: https://dashboard.tic.va.gov/s/28Y/</p> <ul style="list-style-type: none"> • <u>System Owner or Delegate</u> uploads the Compliance Trending and Checklist Trending reports to the Documents tab in RiskVision. • <u>System Owner or Delegate</u> creates one finding and a response in the Findings tab within RiskVision for the compliance scan to serve as a reminder to resolve the deficiencies. • <u>System Owner or Delegate</u> continues to remediate deficiencies identified from the Compliance Trending and Checklist Trending reports. • <u>System Owner or Delegate</u> uploads new Compliance Trending and Checklist Trending reports to the Documents tab within RiskVision as evidence to show the remediation progress. <p>For systems with IP address ranges external to the VA that do not have the IBM Endpoint Manager (IEM) agent installed:</p> <ul style="list-style-type: none"> • <u>System Owner or delegate</u> must submit a 'Supplemental Scan Request' form found at A&A Home Documents to CPO at CertificationPMO@va.gov. Ensure that the 'Compliance' check box is checked. • <u>CPO</u> will submit this form to the NSOC and an NSOC POC will contact the System Owner/Administrator to schedule the compliance scan. 	<p>https://dashboard.tic.va.gov > Enterprise > All Systems > Authorization & Accreditation</p> <ul style="list-style-type: none"> • OCS preferred template location on the OIS Portal at A&A Home Documents
--	--	--	--

		<ul style="list-style-type: none"> • <u>NSOC</u> will submit compliance results/reports to system POCs for compliance scans that are conducted. 	
Requirement		Roles / Responsibilities	References
Security Documentation Requirements			
<input type="checkbox"/>	System Security Plan (SSP) <ul style="list-style-type: none"> • The SSP is developed within RiskVision. • All required diagrams and confirmation of the security authorization boundary to include all devices and supporting software architecture should be included. • All controls must be addressed. A finding will need to be created in RiskVision for every control that is not in place. 	<ul style="list-style-type: none"> • <u>System Steward</u> completes the assessments in RiskVision and develops findings and responses in the Findings tab for controls not in place. • <u>ISO</u> validates information added by the System Steward in RiskVision. • <u>The ISO, System Owner or delegate/System Steward</u> exports the SSP from RiskVision and uploads the document to the Documents tab in RiskVision. 	<ul style="list-style-type: none"> • NIST SP 800-18 and VA Handbook 6500.3 • Additional guidance for completion of the SSP can be provided by OCS
<input type="checkbox"/>	Minor Application Self-Assessment <ul style="list-style-type: none"> • Minor Application Self-Assessment must be completed for all minor applications. 	<ul style="list-style-type: none"> • <u>The ISO, Project team, and the SS</u>, working in conjunction should prepare the Minor Application Security Control Summary and provide implementation detail for all applicable security controls and upload the Self-Assessment to GSS/MA Documents repository in RiskVision. 	<ul style="list-style-type: none"> • Minor Application Self Assessment SOP (Appendix D)
<input type="checkbox"/>	Signatory Authority <ul style="list-style-type: none"> • The Signatory Authority must be signed and dated by the appropriate parties. 	<ul style="list-style-type: none"> • <u>System Owner or delegate</u> completes the Signatory Authority using the template provided at A&A Home Documents and uploads the Signatory Authority to RiskVision under Entity Details: Documents tab. 	<ul style="list-style-type: none"> • NIST SP 800-18 • Additional guidance for completion of the Signatory Authority can be provided by OCS
<input type="checkbox"/>	Risk Assessment (RA) <ul style="list-style-type: none"> • The RA is developed within RiskVision. 	<ul style="list-style-type: none"> • <u>System Steward</u> completes the assessments in RiskVision. • <u>ISO</u> validates information added by the System Steward in RiskVision. • <u>The ISO, System Owner or delegate/System Steward</u> exports the RA from RiskVision and uploads the document to the Documents tab in RiskVision. 	<ul style="list-style-type: none"> • NIST SP 800-30 • Additional guidance for completion of the RA can be provided by the Office of Risk Management and Incident Reporting (RMIR)/OCS
<input type="checkbox"/>	Configuration Management Plan (CMP) <ul style="list-style-type: none"> • The CMP should include processes for managing configuration and change management. • The CMP should include infrastructure devices and baseline configurations (e.g., switches, routers, firewalls). 	<ul style="list-style-type: none"> • <u>System Owner or delegate</u> completes the CMP using the template provided at A&A Home Documents and uploads the CMP as evidence to RiskVision under Entity Details: Documents tab. 	<ul style="list-style-type: none"> • NIST SP 800-70 and VA Handbook 6500 • Additional guidance for completion of the CMP can be provided by OCS

	<ul style="list-style-type: none"> The CMP should include a configuration file for each operating system(s), database(s), application(s), and network device(s) to validate compliance with baseline configuration. 		
<input type="checkbox"/>	Incident Response Plan (IRP) <ul style="list-style-type: none"> The IRP must be created using RA and SSP. The IRP must meet the following standards: <ul style="list-style-type: none"> Information Access and Privacy Program NIST Special Publication 800-61 - Computer Security Incident Handling Guide VA Handbook 6500.3, Certification and Authorization of Federal Information Systems Each site is responsible for developing local level procedures incorporating VA-NSOC areas of responsibility. 	<ul style="list-style-type: none"> <u>System Owner</u> works with the assigned <u>ISO</u> to create the IRP. <u>System Owner or designee</u> uploads the signed IRP into RiskVision once completed and tested. 	<ul style="list-style-type: none"> NIST SP 800-61 Useful tools and websites: <ul style="list-style-type: none"> Agilance RiskVision Enterprise Operations GRC Instance Agilance RiskVision National Release GRC Instance Office of Cyber Security (OCS) Portal
<input type="checkbox"/>	Information Security Contingency Plan (ISCP) <ul style="list-style-type: none"> The ISCP must be created using following inputs: <ul style="list-style-type: none"> Preliminary Information System Contingency Plan Primary Site System Security Plan Backup Site System Security Plan The ISCP must meet the following standards: <ul style="list-style-type: none"> NIST Special Publication 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems Office of Information Security, Authorization Requirements Guide Standard Operating Procedures VA Handbook 6500.8, Information System Contingency Planning 	<ul style="list-style-type: none"> <u>System Owner or delegate</u> develops or revises the Information System Contingency Plan. <u>System Owner or designee</u> uploads the Information System Contingency Plan into RiskVision. 	<ul style="list-style-type: none"> Additional guidance for completion of the ISCP can be provided by the OBC Useful tools and websites: <ul style="list-style-type: none"> Agilance RiskVision Enterprise Operations GRC Instance Agilance RiskVision National Release GRC Instance Business Continuity Portal Office of Cyber Security (OCS) Portal
<input type="checkbox"/>	Disaster Recovery Plan (DRP) <ul style="list-style-type: none"> The DRP must be created using following inputs: <ul style="list-style-type: none"> Primary Site System Security Plan Backup Site System Security Plan The DRP must meet the following standards: <ul style="list-style-type: none"> Office of Information Security, Authorization Requirements Guide Standard Operating Procedures 	<ul style="list-style-type: none"> <u>System Owner or designee</u> develops the DRP as the entry point for the creation of both the facility and data center plans. <u>System Owner or designee</u> uploads the DRP into RiskVision once completed and tested. 	<ul style="list-style-type: none"> Additional guidance for completion of the ISCP can be provided by the OBC Useful tools and websites: <ul style="list-style-type: none"> Agilance RiskVision Enterprise Operations GRC Instance Agilance RiskVision National Release GRC

			Instance <ul style="list-style-type: none"> • Business Continuity Portal • Office of Cyber Security (OCS) Portal
<input type="checkbox"/>	Privacy Impact Assessment (PIA) <ul style="list-style-type: none"> • A complete PIA must have: <ul style="list-style-type: none"> • A previously completed Privacy Threshold Analysis (PTA). <ul style="list-style-type: none"> • Been completed in the most up-to-date and Privacy Services approved template for both the PTA and PIA. The PTA and PIA template can be found at A&A Home Documents • Been completed in coordination with the VA Privacy Services Office. • Been signed by the System Owner, Privacy Officer, and ISO. • Been re-submitted whenever there are major changes to the system or within 3 years. 	<ul style="list-style-type: none"> • <u>System Owner, Privacy Officer, and ISO</u> work together to submit a PTA, which is reviewed by the Privacy Services Office. After review and determination by analysts, the PTA must be signed by the System Owner, Privacy Officer, ISO, and any other relevant stakeholders and re-submitted to the Privacy Services Office via PIASupport@va.gov. If a PIA is required as an outcome of the PTA analysis by the Privacy Services Office, a PIA must be completed and submitted to the Privacy Services Office and then comments by the analysts, if any, must be incorporated. • <u>Privacy Services</u> verifies PIA and provides results. • <u>System Owner or delegate</u> re-submits the PIA as a PDF file with the signatures of the System Owner, Privacy Officer, ISO, and any other relevant stakeholders to PIASupport@va.gov. • <u>System Owner or delegate</u> uploads the PIA to RiskVision under Entity Details: Documents tab. 	<ul style="list-style-type: none"> • Authority is found in E-Government Act of 2002, OMB Circular 03-22, VA Directive 6502, VA Directive 6508, and VA Handbook 6508.1 • Additional guidance for completion of the PIA/PTA can be provided by the Privacy Services Office. Any questions may be sent to PIASupport@va.gov
<input type="checkbox"/>	Interconnection Security Agreement (ISA)/ Memorandum of Understanding (MOU) <ul style="list-style-type: none"> • An ISA/MOU must be provided for all external interconnections. 	<ul style="list-style-type: none"> • <u>System Owner</u> in coordination with the entities identified in NIST SP 800-47 will complete the ISA/MOU using the latest template provided at: OIS Portal or A&A Home Documents. • <u>ISO</u> will upload all final draft MOU/ISA documents to the MOU/ISA Review Submissions SharePoint site for a review prior to requesting signatures. • <u>VA review team</u> will assess the documents against a checklist for quality and content. • <u>Reviewer and the ISO</u> will work collaboratively to correct deficiencies found in the documentation. • <u>Reviewer</u> will notify the ISO via email informing them that the document is ready for signatures. • <u>ISO</u> will process the document for signature. • <u>ISO</u> will upload the document to the Enterprise Document SharePoint upon receipt of the completed and signed MOU/ISA document,. 	<ul style="list-style-type: none"> • NIST SP 800-47, VA Handbook 6500, and FSS Bulletin#269 • Additional guidance can be provided by the Health Information Security Division at vafsshisd@va.gov or the OIT ERM CRISP Team at Sharon.mcallister@va.gov



		<ul style="list-style-type: none">• The finalized document should also be added to the existing A&A artifacts in RiskVision.	
--	--	--	--

Appendix C – Job Aid: Security Information

Job Aid

Security Information

1. Purpose

This Job Aid will assist Information Security Officers (ISOs), Facility Chief Information Officers (FCIOs), System Owners and stakeholders with security responsibilities when performing security-related job functions. The Job Aid provides security information on the following items:

- Authorization Decision Process
- VA Authorization Boundaries
- Finding/Milestone Process
- Vulnerability Integration into Authorization Decision Process
- NIST SP 800-53 Rev 3 to Rev 4 Transition

This Job Aid is subject to change as new critical security elements emerge and/or VA policies and processes change.

2. Authorization Decision Process

Independent third-party Assessment & Authorization (A&A) reviews are conducted to determine the technical security posture of VA's Information Technology (IT) systems. A&A reviews evaluate all applicable system security controls conducted in accordance with the Authorization Requirements Guide / Standard Operating Procedure (SOP). A&A reviews include a combination of:

- On-site assessments conducted by Enterprise Risk Management (ERM) on a sub-set of VA systems and Managed Services.
- Technical security tests (penetration tests, vulnerability scans, discovery scans, and security configuration compliance scans) conducted by the VA-NSOC.
- Verification and Validation (V&V) Secure Code Reviews conducted by VA Application Developers.
- Office of Cyber Security (OCS) third-party assessments of all system security documentation, on-site assessment results, technical testing results, secure code review results, and configuration files provided by the system personnel.

All VA systems were assessed in August 2013 during the deployment of RiskVision. If a package lacked information but the security posture was acceptable, the Authorizing Official could issue an ATO with Conditions, thereby allowing the system to store, process, or transmit VA data, while the remaining

security information is provided by the System Owner. Under no circumstances, has any VA system been allowed to operate minus a review of the security authorization package required by NIST. It is important to note the NIST affords Federal Departments and Agencies latitude throughout the authorization process to make balanced decisions that are based on security risk and the business needs of the Department. It is incorrect to state that VA systems were not assessed consistent with NIST standards and were allowed to operate devoid of a security posture determination.

VA authorization requirements can be conducted and met using remote capabilities. Therefore, on-site SCAs conducted by ERM are only conducted on a sub-set of VA systems annually. This is also in part due to lack of resources, funding, and time required to travel to VA and Managed Service sites. The schedule for system SCAs is determined by ERM in coordination with OCS based on available resources, budget, and system SCA needs.

All VA systems are required, and were required upon the issuance of new authorization boundaries, to address the VA Authorization requirements in accordance with the Authorization Requirements SOP / Guide and VA Handbook 6500.

Reference 1: Authorization Requirements Standard Operating Procedure (SOP) / Guide – [A&A Home Documents](#)

Reference 2: ERM SCA Results are uploaded to RiskVision under the respective system as well as at the following location – [SCA Assessment Results](#)

Reference 3: DAS Expectation Memo: Authorization Requirements Expectations (March 19, 2014)

3. VA Authorization Boundaries

The authorization boundaries were changed in the summer of 2013 to meet OIS strategic goals, improve accountability, better define common controls, and align with actual operational and managerial practices. The system boundaries for the three major systems cover the entire Region; there are no facility-level boundaries although there are facility-level controls, and RiskVision maps each known IP address to the system that contains it. System security documentation was updated / re-created to reflect the new authorization boundaries in August 2013 and assessed as a part of the OCS third-party assessments. If the security documentation lacked information but the security posture of the system was acceptable (according to technical testing results, other security artifacts, etc.), the Authorizing Official could issue an ATO with Conditions thereby allowing the system to store, process, or transmit VA data, while the remaining security information was provided by the System Owner. Any SSPs that are incomplete and do not appropriately reflect the authorization boundaries are required to be updated as a condition of the authorization process. In all cases, any gaps in the documentation are thoroughly assessed to determine their impact on the authorization decision.

The system boundaries have been reviewed and approved by the Certification Authority and the Authorizing Official (AO). The three primary systems / authorization boundaries are as follows:

- VistA - Composed of VistA Mumps environment and its applications, and user data sorted in 'dat' files. This system boundary will not contain IP addresses or operating systems only the Major Application.

- GSS - Composed of desktops, laptops, file/print servers, COTS and other applications including operating systems. IP addresses are used to define this boundary.
- Infrastructure - Composed of local area networking equipment that connects the other two including, routers, switches, firewalls, load balancers, wireless access points. IP addresses are used to define this boundary.

The authorization boundaries are based on NIST 800-18 and summarized in the System Security Plan (SSP) while RiskVision contains a more thorough definition of the boundaries; down to the IP address level. All established IP addresses in VA are assigned to a system boundary and RiskVision contains a list of these IP assignments. Maintaining a current list of IP addresses in the SSP is impractical due to the frequency of IP address changes. Therefore, the SSP boundary description is a high-level depiction while RiskVision's boundary description includes components down to the device level.

Note: Facility-level staff are no longer System Owners. Any questions concerning system boundaries should be referred to the Regional System Owner if facility staff are unable to provide a detailed answer.

4. Finding/Milestone Process

RiskVision allows for granular identification and remediation of Findings (aka POA&Ms), accountability, and tracking mechanisms by management. Open Findings are assigned at the entity level to which the control is presented. This means that findings can be presented at a Region entity, GSS Information System, Infrastructure Information System, Vista Information System or facility level. ISOs are required to conduct reviews of the security control implementation statements and create a Finding in RiskVision, with an associated milestone, for controls that are not properly implemented in accordance with VA and Federal guidance. January CRISP Focus training and multiple ISO and SDE GRC training opportunities and guidance were provided to assist with the creation of Findings and milestones.

Per the Authorization Requirements SOP and Authorization Requirements training, a Finding should be created by system personnel within RiskVision to track the vulnerabilities identified from scans. The field is required to develop a remediation plan for the vulnerabilities.

POA&M Transition from SMART to RiskVision

POA&Ms in SMART dated back as early as 2005. With the implementation of RiskVision, VA is able to capture more relevant information on compliance and security data within IBM Endpoint Manager (IEM) and Nessus. Also, the new authorization boundaries cause the pre-existing SMART POA&Ms to be irrelevant and outdated; with the exception to the 2012 and 2013 OIG findings which were migrated over to RiskVision. Also, controls that may have been the target during a 2012 facility audit may now only be present at an information system level. With the transformation of the A&A process and its focus on technical security requirements, as opposed to paper based processes (which many of the pre-existing POA&Ms were based on), VA is now able to better articulate the security posture of its information systems.

Reference 1: [CRISP FOCUS SharePoint](#)

Reference 2: [Executive Decision Memorandum – FISMA Challenge Recommendations](#)

5. Vulnerability Integration into Authorization Decision Process

In accordance with the Authorization Requirements Standard Operating Procedure (SOP) / Guide, OCS assesses vulnerabilities identified through the following tests / scans provided in RiskVision by system personnel prior to T/ATO issuance:

- NSOC Penetration Tests
- NSOC Vulnerability Scans / Discovery Scans
- Security Configuration Compliance Scans
- Secure Code Reviews

All VA systems were assessed in August 2013 during the deployment of RiskVision. If a package lacked vulnerability information but the security posture was acceptable (according to existing technical testing results, security documentation, etc.), the Authorizing Official can issue an ATO with Conditions thereby allowing the system to store, process, or transmit VA data, while the remaining security information is provided by the System Owner. As new vulnerability scans / technical tests are conducted on systems, they are re-assessed for a new authorization decision based on the current security state.

The field is required to develop a remediation plan of the vulnerabilities along with an expected completion date, and upload the information to RiskVision. This involves the system personnel analyzing the deficiencies to determine which are applicable to their authorization boundary, identifying false positives, providing a remediation strategy (using various methods), and also providing an expected completion date for remediation. In addition, system personnel have the responsibility of providing updated information and remediation strategies in RiskVision. OCS may follow-up for additional information when necessary. The controls associated with technical scanning are not presented to the facility level but rather the Information System level.

The results of OCS assessments are provided in the T/ATO recommendation that is submitted to the Authorizing Official (AO), the VA Chief Information Officer, for the final authorization decision. OCS provides an explanation of the existing vulnerabilities, the potential risk the vulnerabilities bring to the VA network, as well as conditions that the system needs to address relative to the closure of the vulnerabilities.

[Importing Scan Data into RiskVision](#)

RiskVision imports Nessus scan data from NSOC via the Threat & Vulnerability Manager (TVM). Nessus scan data was imported and made available to the field on April 1, 2014. TVM training was provided to the field on March 26 and 27, 2014.

Reference 1: Authorization Requirements Standard Operating Procedure (SOP) / Guide – [A&A Home Documents](#)

Reference 2: [TVM Training](#)

6. NIST SP 800-53 Rev 3 to Rev 4 Transition

OIS Risk Based Decision (RBD) 53, Implementation of NIST 800-53 Revision 4 is in place acknowledging that VA has not issued updated policy guidance that adds the new Revision 4 requirements. However,

OMB guidance (M-04-14) provides Departments with the flexibility and latitude in applying and implementing NIST's guidelines. VA will apply the NIST Rev 4 guidance to all new system implementations and also when systems undergo upgrades. This is standard practice throughout the government for several years and accepted by OIGs at other Departments. It is not practical or cost effective to immediately update all systems within one year, each time NIST updates its systems security guidelines. The new Revision 4 adds 200 new additional system security controls or enhancements for federal systems. For VA legacy systems in operation and not due for upgrades, VA will consider using RBDs regarding whether it is cost effective to implement out of cycle upgrades to address new NIST systems security guidance.

The updated VA Handbook 6500 reflecting NIST Revision 4 has been drafted and is currently going through the concurrence process, and is expected for release prior to the end of the 2014 fiscal year. OIS is taking action to expedite the policy coordination and issuance process to make it timelier for future policy updates. An RBD or POA&M/Finding will be developed for legacy systems that are not due for upgrades, to assess whether the systems development life cycle process will support the implementation of new, additional controls.

RiskVision will be capable of performing assessments based on Revision 4 content by June 30, 2014, with new assessments being conducted consistent with Revision 4 by the end of the 1st Quarter of FY15.

Appendix D – Minor Applications Self-Assessment SOP

Purpose

The purpose of this Standard Operating Procedure (SOP) is to provide guidelines for the Security Authorization process of Minor Application(s) that are listed under a General Support System (GSS) or Major Application (MA). The SOP establishes procedures for incorporating the Minor Application Security Controls Summary document into the local site's Compliance Report for the parent GSS or Major Application to ensure the security and integrity of the VA's information systems are maintained. In general, a Minor Application is an application that is not a standalone application, or is a component of a MA or GSS, and receives much of its security from the parent application or system.

The process determines the extent to which the security controls are implemented correctly, operating as intended, and producing desired outcome with respect to meeting security requirements. Each listed control is designed to determine the sufficiency and effectiveness of a controlled feature or safeguard. Not all controls are applicable to all Minor Applications.

Scope

The scope of the Minor Application Security Controls Summary process covers only the minor application under evaluation, including connectivity within the system. Evaluation will be conducted in the areas of:

- Access Control
- Audit and Accountability
- Security Authorization and Security Assessments
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning, Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection and
- System and Information Integrity

Note: Incident Response and Awareness and Training are covered by the GSS or Major Application in their entirety

Procedure

In accordance with Federal Information Processing Standard (FIPS) 199 Standards for Security Categorization of Federal Information and Information Systems, security categorization for both information and information systems is calculated based on the three basic security objectives; confidentiality, integrity, and availability. National Institute of Standards and Technology (NIST) Publication 800-60 Guide for Mapping Types of Information and Information System to Security Categories provides implementation guidance in completing this activity.

* Minor Applications cannot have a Security Category higher than that of the host system.

- |||||
1. If the application falls under a GSS or Major Application and is considered a Minor Application, then the Minor Application Security Control Summary can be used in place of an SSP. The List of Security Controls of this SOP shall also be used to document the security controls as they are implemented for a specific application. The Minor Application Self-Assessment Workbook can be found at [A&A Home Documents](#).
 2. The ISO, Project Team and the SS, working in conjunction, should prepare the Minor Application Security Control Summary and the List of Security Controls.
 - Only those controls that are provided by the Minor Application need a complete implementation explanation, annotated and shall be documented just as they would be if an SSP were required.
 - Controls that are provided by the host system, whether it is a MA or GSS should be annotated as such.
 - There is no need to annotate common controls, (Those controls are managed at the enterprise level) and they have been eliminated from the list of security controls in order to avoid duplication of effort.
 - If the control cannot be implemented, it is neither a common control nor a control that is being provided by the host system, it must be noted.
 3. The Minor Application Security Control Summary shall be inserted as an appendix to hosting GSS/MA SSP. The application should be identified in the SSP table of content as a Minor Application under GSS or MA.

Monitoring

The ISO will store all records developed throughout this process in the Documents repository within RiskVision of the MA or GSS which supports this Minor Application. Additionally, the ISO conducts audits and/or actions as directed by Continuous Readiness Information Security Program (CRISP) action items and any additional mandated VA policy or guidance.

Definitions

Authorization: The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

Authorizing Official: Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.

Business Requirements Document (BRD): The Business Requirements Document (BRD) is authored by the business community for the purpose of capturing and describing the business needs of the customer/business owner. The BRD provides insight into the AS IS and TO BE business area, identifying stakeholders and profiling primary and secondary user communities. This document identifies what capabilities the stakeholders and the target users need and why these needs exist, providing a focused overview of the request requirements, constraints, and Information Technology (IT) options to be considered. This document does not state the development methodology.

Common Security Control: Security control that can be applied to one or more agency information systems and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the security certification and authorization processes of an agency information system where that control has been applied.

Compensating Security Controls: The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST SP 800-53, Latest Version, that provide equivalent or comparable protection for information systems and the information processed, stored, or transmitted by those systems.

EIB Milestone 0: Enterprise Information Board (EIB0 Milestone 0 is intended to have the Contracting Officer, Contracting Officer Representative, or Project Manager address the basic areas necessary to warrant project initiation approval. It does not presume any significant prior investment in analysis (either business or technical), concept or requirements definition or design; rather, it seeks answers to these most basic questions even before committing to that level of investment. The Project Manager should have a clear understanding of the problem that needs to be solved and how solving that problem supports a strategic objective of the Department. Based on a successful Milestone 0 review, the Project Manager will be authorized to expend the resources necessary to establish the project's business case and prepare for the project's Milestone I review.

General Support System: An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

High Impact System: An information system in which a least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.

Information Owner: Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information Security: A means for protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

Information Security Officer (ISO): Individual responsible to the senior agency information security officer, authorizing official, or information system owner for ensuring the appropriate operational security posture is maintained for an information system or program.

|||||

Information Security Requirements: Information security requirements promulgated in accordance with law, or directed by the Secretary of VA, the National Institute of Standards and Technology, and the Office of Management and Budget, and, as to national security systems, the President.

Information Sensitivity: Information sensitivity reflects the relationship between the characteristics of the information processed (e.g., personnel data subject to protection under the Privacy Act) and the mission need to ensure the confidentiality, integrity, and availability of the information (e.g., legal requirements to protect confidentiality of personal data). Sensitivity may vary from low, to medium, to high.

Information System Owner: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Information Type: A specific category of information, (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization, or in some instances, by a specific law, executive order, directive, policy or regulation.

Low Impact System: An information system in which all three security objectives (i.e. confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.

Major Application: An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

Minor Application: An application can be classified as being a Minor Application if they meet the following conditions: they rely upon a General Support System (GSS) or Major Application for security, they are within another system's authorization boundary, and they do not have their own capital plan.

Moderate Impact System: An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high.

Potential Impact: The loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect (FIPS 199 low); (ii) a serious adverse effect (FIPS 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.

Security Category: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.

Security Controls: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

System Security Plan: Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

References

- 5 U.S.C. 552a, Privacy Act, c. 1974
- 38 U.S.C. 5705, Confidentiality of medical quality assurance records.
- Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems.
- VA Directive 6500, Information Security Program
- VA Handbook 6500, Information Security Program
- VA Directive 6001, Limited Personnel Use of Government Office Equipment Including Information Technology
- OMB Circular A-123 II, Management Accountability and Control,
- NIST SP 800-37 “Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life cycle Approach”
- NIST SP 800-53, “Recommended Security Controls for Federal Information Systems”
- NIST SP 800-53A, “Guide for Assessing the Security Controls in Federal Information Systems”
- Records Management, FSS Records Management
- FIPS Publication 199, “Standards for Security Categorization of Federal Information and Information Systems”

Appendix E – A&A System/Facility DRP and ISCP Requirements

<i>Boundary</i>	<i>Plans</i>	<i>DRP</i>	<i>Comments</i>
<i>Region1</i>	<ul style="list-style-type: none"> • Region 1 - RCSnet Assessing • Region 1 GSS Assessing • Region 1 Infrastructure Assessing • Region 1 VistA Assessing 	Facility DRPs (collectively) cover the Region DRP requirement	ISCP plan expected for each assessing entity as identified in GRC
<i>Region2</i>	<ul style="list-style-type: none"> • Region 2 GSS Assessing • Region 2 Infrastructure Assessing • Region 2 VistA Assessing 	Facility DRPs (collectively) cover the Region DRP requirement	ISCP plan expected for each assessing entity as identified in GRC
<i>Region3</i>	<ul style="list-style-type: none"> • Region 3 GSS Assessing • Region 3 Infrastructure Assessing • Region 3 VistA Assessing 	Facility DRPs (collectively) cover the Region DRP requirement	ISCP plan expected for each assessing entity as identified in GRC
<i>Region4</i>	<ul style="list-style-type: none"> • Region 4 Infrastructure Assessing • Region 4 VistA Assessing • Region 4 - Electronic Computer Access Request (eCAR) Assessing • Philadelphia – BHIE Assessing 	Facility DRPs (collectively) cover the Region DRP requirement	ISCP plan expected for each assessing entity as identified in GRC
<i>Region5</i>	<ul style="list-style-type: none"> • Region 5 GSS Assessing • Region 5 Infrastructure Assessing 	Facility DRPs (collectively) cover the Region DRP requirement	ISCP plan expected for each assessing entity as identified in GRC



<i>Region6</i>	<ul style="list-style-type: none">• Region 6 GSS Assessing• Region 6 Infrastructure Assessing• Region 6 - CDB Assessing• Region 6 VistA Assessing• Region 6 - FPPS Assessing• Region 6 - WRAP Assessing• Region 6 - CIRTSS Assessing• Region 6 - OSCRA Assessing• Region 6 – VHALWD Assessing	Facility DRPs (collectively) cover the Region DRP requirement	ISCP plan expected for each assessing entity as identified in GRC
<i>Facilities</i>	<ul style="list-style-type: none">• Facility. LAN.ISCP• Facility. PBX.ISCP (May only apply to certain facilities with wired PBX)• Facility. Major application (May only apply to facility that house and manage the MA)• Facility.DRP	Each facility must have a DRP plan	ISCP plan expected for LAN and as applicable PBX and or MA
<i>Region Other</i>	Each GRC Assessing entity must have an ISCP plan	Each GRC Assessing entity must have a DRP plan	ISCP plan expected for each assessing entity as identified in GRC

Appendix F – Links/URLs/E-Mail Addresses

Links & URLs	
Short Links	Full Address
(FSS) Bulletin #124 (MOU/ISA Guidance)	https://vaww.portal2.va.gov/sites/infosecurity/fieldsecurity/FSS%20Bulletins/124_MOU%20ISA%20Document%20Processing%20FINAL%20Guidance_080113.pdf
A&A Home Documents	https://vaww.portal2.va.gov/sites/infosecurity/ca/CA%20Home%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Finfosecurity%2Fca%2FCA%20Home%20Documents%2FVA%20A%20and%20A%20Templates&FolderCTID=0x012000CB0DD849BEA0AB4FA5FEE491047C852D&View={5FCA9CEF-1C50-441D-A2FE-28D536ED0098}
Acceptance of FEDRAMP Authorization Memo	https://vaww.sde.portal.va.gov/docctr/Memoranda/150811-005R-Acceptance_of_FEDRAMP_Authorizations.pdf
Approved Security Directives and Handbooks	https://vaww.portal2.va.gov/sites/infosecurity/ca/policy_default.aspx
Authorization Requirements Quick Link Reference Guide	https://vaww.portal2.va.gov/sites/infosecurity/ca/CA%20Home%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Finfosecurity%2Fca%2FCA%20Home%20Documents%2FATO%20Documents&FolderCTID=0x012000CB0DD849BEA0AB4FA5FEE491047C852D&View={5FCA9CEF-1C50-441D-A2FE-28D536ED0098}
Business Continuity Portal	https://vaww.portal2.va.gov/sites/infosecurity/bc/default.aspx
Common Application Enumeration	https://wiki.mobilehealth.va.gov/display/OISSWA/Common+Application+Enumeration
CRISP FOCUS SharePoint	https://vaww.portal2.va.gov/sites/infosecurity/iprm/OIS%20Communications%20Home%20Folder%201/Forms/AllItems.aspx?RootFolder=/sites/infosecurity/iprm/OIS%20Communications%20Home%20Folder%201/CRISP%20FOCUS%20Campaign/Year%20Five&FolderCTID=0x0120004841CB7EF061244DBC5BD867B86555D1&View=%7b0F93DBB4-6AA1-4A48-95F1-D1C9735AFF78%7d
Enterprise Operations GRC Instance	https://vaww.eogrc.va.gov/spc/index.jsp
Enterprise Visibility and Vulnerability Management (EVVM) Dashboard	https://dashboard.tic.va.gov
Executive Decision Memorandum – FISMA	https://vaww.portal2.va.gov/sites/infosecurity/iprm/OIS%20Communications%20Home%20Folder%201

Challenge Recommendations	/Memoranda/EDM%20-%20FISMA%20Challenge.pdf
FedRAMP-Agency Access Request Form	https://www.fedramp.gov/assets/resources/documents/Agency_Package_Request_Form.pdf
Information Access and Privacy Program	https://vaww.vets.vaco.portal.va.gov/sites/privacy/Pages/default.aspx
ISA/MOU Document Review Site	https://vaww.portal2.va.gov/sites/infosecurity/ca/CA%20Home%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Finfosecurity%2Fca%2FCA%20Home%20Documents%2FVA%20A%20and%20A%20Templates&FolderCTID=0x012000CB0DD849BEA0AB4FA5FEE491047C852D&View=%7b5FCA9CEF-1C50-t
ISCP/DRP Template	https://vaww.portal2.va.gov/sites/infosecurity/bc/ISCPA%20Process%20Documentation/Forms/AllItems.aspx
National Release GRC Instance	https://vaww.grc.va.gov/spc/index.jsp
NIST Special Publication 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems	http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf
NIST Special Publication 800-61 - Computer Security Incident Handling Guide	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
NSOC Scan Documents	https://vaww.portal2.va.gov/sites/infosecurity/ca/CA%20Home%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Finfosecurity%2Fca%2FCA%20Home%20Documents%2FCSOC%20Scan%20Documents&FolderCTID=0x012000CB0DD849BEA0AB4FA5FEE491047C852D&View=%7B5FCA9CEF-1C50-441D-A2FE-28D536ED0098%7D
Office of Cyber Security (OCS) Portal	https://vaww.portal2.va.gov/sites/infosecurity/ca/default.aspx
Office of Information Security (OIS) Portal	https://vaww.portal2.va.gov/sites/infosecurity/index.aspx
Office of Information Security, Authorization Requirements Guide Standard Operating Procedures	https://vaww.portal2.va.gov/sites/infosecurity/ca/CA%20Home%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Finfosecurity%2Fca%2FCA%20Home%20Documents%2FATO%20Documents&FolderCTID=0x012000CB0DD849BEA0AB4FA5FEE491047C852D&View={5FCA9CEF-1C50-441D-A2FE-28D

POA&M Management Guide	https://vaww.portal2.va.gov/sites/infosecurity/ca/CA%20Home%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Finfosecurity%2Fca%2FCA%20Home%20Documents%2FATO%20Documents&FolderCTID=0x012000CB0DD849BEA0AB4FA5FEE491047C852D&View=%7b5FCA9CEF-1C50-441D-A2FE-28D
Request For Information Security Officer Support Form	https://vaww.portal2.va.gov/sites/infosecurity/ca/CA%20Home%20Documents/ATO%20Documents/FSS_ISO%20Support_Request.pdf
SCA Assessment Results	https://vaww.portal2.va.gov/sites/infosecurity/projects/SCA%20Assessments/Lists/SCA%20Assessment%20Results/AllItems.aspx
Training and Brown Bag Materials	https://vaww.portal2.va.gov/sites/infosecurity/projects/GRC%20Tool/GRC%20Tool%20Training%20Materials/Forms/AllItems.aspx
TVM Training	https://vaww.portal2.va.gov/sites/infosecurity/projects/GRC%20Tool/GRC%20Tool%20Training%20Materials/Forms/AllItems.aspx?RootFolder=/sites/infosecurity/projects/GRC%20Tool/GRC%20Tool%20Training%20Materials/TVM%20Training&FolderCTID=0x012000C5851A4D870A2F49AC5BFED7E758CE1F&View=%7b27EC8AEE-0BCC-4C7D-88E7-F5321F82F5EC%7d
VA Directive 6404	http://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=826&FTYPE=2
VA Handbook 6500.3, Certification and Authorization of Federal Information Systems	http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=733&FTYPE=2
VA Software Assurance Developer Support	https://wiki.mobilehealth.va.gov/display/OISSWA/How+to+open+an+NSD+ticket+to+register+a+VA+application
VA SwA Program Office Resource	https://wiki.mobilehealth.va.gov/display/OISSWA/OIS+Software+Assurance
E-Mail Addresses	
Name	E-Mail
Certification Program Office	CertificationPMO@va.gov
Enterprise Visibility Team	OISEVSupportGroup@va.gov
FSS Health Information Security Division	vafsshisd@va.gov
OIT Enterprise Risk Management (ERM) CRISP Team	Sharon.mcallister@va.gov
Privacy Services Office	PIASupport@va.gov



VA FSS ISO Request	VAFSSISORequests@va.gov
VA GRC Service Desk	vaGRCservicedesk@va.gov
VA RiskVision Working Group (RVWG)	VARiskVisionWG@va.gov
VA Software Assurance (SwA) Program Office	OISSwASupportGroup@va.gov